Takatoshi, Ono et al.

#2

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

NAK1:BK74

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: １９９９年 ４月２７日

出 願 番 号
Application Number: 平成１１年特許願第１１９４４２号

出 願 人
Applicant (s): 松下電器産業株式会社

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年 ３月３１日

特 許 庁 長 官
Commissioner,
Patent Office 近 藤 隆 彦

出証番号 出証特２０００－３０２２９８７

【書類名】　特許願

【整理番号】　2022510233

【提出日】　平成11年 4月27日

【あて先】　特許庁長官殿

【国際特許分類】　G06F 9/06

G09C 1/00

【発明者】

【住所又は居所】　愛知県名古屋市中区栄２丁目６番１号白川ビル別館５階
株式会社松下電器情報システム名古屋研究所内

【氏名】　小野　貴敏

【発明者】

【住所又は居所】　大阪府門真市大字門真１００６番地　松下電器産業株式会社内

【氏名】　原田　俊治

【特許出願人】

【識別番号】　000005821

【氏名又は名称】　松下電器産業株式会社

【代理人】

【識別番号】　100097445

【弁理士】

【氏名又は名称】　岩橋　文雄

【選任した代理人】

【識別番号】　100103355

【弁理士】

【氏名又は名称】　坂口　智康

【選任した代理人】

【識別番号】　100109667

【弁理士】

【氏名又は名称】　内藤　浩樹

【手数料の表示】

【予納台帳番号】　011305

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9809938

【プルーフの要否】　不要

【書類名】　明細書

【発明の名称】　デジタルコンテンツ利用制御システム

【特許請求の範囲】

【請求項１】　予め定められた利用条件に従ってデジタルコンテンツの利用を制御し、かつ当該利用条件、当該デジタルコンテンツの不正な使用を防止するためのデジタルコンテンツ利用制御システムであって、

複数の、デジタルコンテンツ、暗号化された利用条件及び暗号化された補助鍵を格納し、かつ情報の読み出し及び書き込みが可能な記録媒体が、デジタルコンテンツを利用する実行器に情報伝達可能に接続され、

前記実行器は、

乱数を格納し、かつ自己の外部からは情報の読み出し及び書き込みが困難な乱数格納手段と、

前記記録媒体から暗号化された補助鍵を獲得して、前記乱数格納手段から取得した乱数で復号する第１の復号手段と、

前記記録媒体から暗号化された利用条件を獲得して、前記第１の復号手段の復号によって得られた補助鍵で復号する第２の復号手段と、

前記記録媒体から対応するデジタルコンテンツを獲得して、前記第２の復号手段の復号によって得られた利用条件に従って利用を実行するデジタルコンテンツ利用手段と、

前記第１の復号手段の復号によって得られた補助鍵とは異なる新たな補助鍵を生成する補助鍵生成手段と、

前記第２の復号手段の復号によって得られた利用条件を、前記デジタルコンテンツ利用手段がデジタルコンテンツを利用した後に、前記補助鍵生成手段によって生成された新たな補助鍵で暗号化して、前記記録媒体に格納する第１の暗号化手段と、

デジタルコンテンツの利用に関連して、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号する第３の復号手段と、

前記第３の復号手段の復号に連携して、前記乱数格納手段に格納された乱数を更

新する乱数更新手段と、

前記第３の復号手段の復号によって得られた補助鍵から、前記第１の復号手段にの復号によって得られた補助鍵を除き、さらに前記補助鍵生成手段によって生成された補助鍵を加えたものを、前記乱数更新手段によって更新された乱数で暗号化して、前記記録媒体に格納する第２の暗号化手段とを備える、デジタルコンテンツ利用制御システム。

【請求項２】　デジタルコンテンツの利用にともなって、前記第２の復号手段の復号によって得られた利用条件を更新する利用条件更新手段をさらに備え、

前記第１の暗号化手段は、前記利用条件更新手段によって更新された利用条件を、前記補助鍵生成手段によって生成された新たな補助鍵で暗号化して、前記記録媒体に格納することを特徴とする、請求項１に記載のデジタルコンテンツ利用制御システム。

【請求項３】　前記第３の復号手段は、デジタルコンテンツの利用毎に、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号することを特徴とする、請求項１または２に記載のデジタルコンテンツ利用制御システム。

【請求項４】　前記補助鍵生成手段は、予め決められた複数回のデジタルコンテンツの利用に一度、前記第１の復号手段の復号によって得られた補助鍵とは異なる新たな補助鍵を生成し、

前記第１の暗号化手段は、予め決められた複数回のデジタルコンテンツの利用に一度、利用条件を前記補助鍵生成手段によって生成された新たな補助鍵で暗号化して、それ以外の時には、前記第１の復号手段の復号によって得られた補助鍵で暗号化して、

前記第３の復号手段は、予め決められた複数回のデジタルコンテンツの利用に一度、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号することを特徴とする、請求項１または２に記載のデジタルコンテンツ利用制御システム。

【請求項５】　前記補助鍵生成手段は、予め決められた可変の回数のデジタルコンテンツの利用に一度、前記第１の復号手段の復号によって得られた補助鍵と

は異なる新たな補助鍵を生成し、
前記第１の暗号化手段は、予め決められた可変の回数のデジタルコンテンツの利用に一度、利用条件を前記補助鍵生成手段によって生成された新たな補助鍵で暗号化して、それ以外の時には、前記第１の復号手段の復号によって得られた補助鍵で暗号化して、
前記第３の復号手段は、予め決められた可変の回数のデジタルコンテンツの利用に一度、前記記録媒体から全ての暗号化された補助鍵を獲得して、前記乱数格納手段に格納された乱数で復号することを特徴とする、請求項１または２に記載のデジタルコンテンツ利用制御システム。

【請求項６】　前記補助鍵生成手段が補助鍵を生成する間隔に関する情報を、デジタルコンテンツ利用者に秘密にすることを特徴とする、請求項５または６に記載のデジタルコンテンツ利用制御システム。

【請求項７】　前記乱数格納手段は、前記実行器に設けられる代わりに、前記記録媒体に設けられることを特徴とする、請求項１または２に記載のデジタルコンテンツ利用制御システム。

【請求項８】　前記記録媒体の代わりに、読み出し専用の第１の記録媒体と、読み出し及び書き込みが可能な第２の記録媒体とが前記実行器に接続され、
前記第１の記録媒体はデジタルコンテンツを格納し、前記第２の記録媒体は暗号化された利用条件を格納し、
前記乱数格納手段は、前記実行器に設けられる代わりに、前記第２の記録媒体に設けられることを特徴とする、請求項１または２に記載のデジタルコンテンツ利用制御システム。

【請求項９】　前記記録媒体に格納されたデジタルコンテンツは、それぞれ暗号化されており、
前記デジタルコンテンツ利用手段は、前記記録媒体から、対応する暗号化されたデジタルコンテンツを獲得して、前記第２の復号手段の復号によって得られた利用条件に従って復号し、復号して得たデジタルコンテンツの利用をを実行することを特徴とする、請求項１または２に記載のデジタルコンテンツ利用制御システム。

【請求項１０】　前記実行器は個々の実行器に固有の実行器固有鍵を持ち、前記デジタルコンテンツ利用手段は、暗号化されたデジタルコンテンツの復号に、前記実行器固有鍵を用いることを特徴とする、請求項９に記載のデジタルコンテンツ利用制御システム。

【請求項１１】　前記デジタルコンテンツ利用手段は、暗号化されたデジタルコンテンツと、その復号に用いる鍵を獲得して、その利用を実行することを特徴とする、請求項９または１０に記載のデジタルコンテンツ利用制御システム。

【請求項１２】　前記乱数更新手段は、前記乱数格納手段に格納された乱数を種に、新たな乱数を生成することを特徴とする、請求項１または２に記載のデジタルコンテンツ利用制御システム。

【請求項１３】　前記乱数更新手段は、前記乱数格納手段に格納された乱数をインクリメントした値を新たな乱数とすることを特徴とする、請求項１または２に記載のデジタルコンテンツ利用制御システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、デジタルコンテンツ利用制御システムに関し、より特定的には、デジタルコンテンツの不正使用を防止するためのデジタルコンテンツ利用制御システムに関する。

【０００２】

【従来の技術】

近年、著作権のある情報のデジタル化が進んでいる。特に音楽情報などはデジタル化を行なうことによって音質の劣化を防ぐことができるという利点がある。しかしデジタル化することによって、不正な利用（複製）が簡易に行なわれてしまうという欠点も表面化している。

【０００３】

このような不正を防ぐためにに、著作権法などの法整備とともに、デジタルコンテンツの利用制御システムが考案されている。例えば、特開平９－１８５５０１号公報には、デジタルコンテンツの一つであるソフトウェアについて、不正に

コピーされたソフトウェアを利用（実行）できないようにする、ソフトウェア実行制御システムが開示されている。

【０００４】

図５は特開平９－１８５５０１号公報に係わるソフトウェア実行制御システムの構成を示すブロック図である。図５において、このシステムは、ソフトウェアを格納する記録媒体２０と、ソフトウェアを実行する実行器２１とを備えている。実行器２１は、乱数格納部２２と、第１の復号部２３と、第２の復号部２４と、第３の復号部２５と、実行回数検査部２６と、実行回数更新部２７と、第１の暗号部２８と、ソフト実行部２９とを含む。

【０００５】

図６は、図５のソフトウェア実行制御システムの動作を示すフローチャートである。図６を用いて、図５に示すシステムの動作を説明する。記録媒体２０には、ソフトウェアＳｏｆｔＡに関する情報として、暗号化ソフトＥ（ＫＡ，ＳｏｆｔＡ）と、暗号化ソフト鍵／実行回数Ｅ（ＲＡ，（ＫＡ，ｎＡ））と、暗号化補助鍵Ｅ（Ｒ，ＲＡ）とが、ソフトウェアＳｏｆｔＢに関する情報として、暗号化ソフトＥ（ＫＢ，ＳｏｆｔＢ）と、暗号化ソフト鍵／実行回数Ｅ（ＲＢ，（ＫＢ，ｎＢ））と、暗号化補助鍵Ｅ（Ｒ，ＲＢ）とが、格納されている。ここで、ＲＡ及びＲＢは、それぞれソフトウェアＳｏｆｔＡ及びソフトウェアＳｏｆｔＢに専用の補助鍵であり、Ｅ（Ｒ，ＲＡ）及びＥ（Ｒ，ＲＢ）は、これらをそれぞれ乱数Ｒで暗号化したものである。

【０００６】

乱数格納部２２は、読み出し及び書き込みの困難な領域であり、乱数Ｒを格納している。実行器２１は、記録媒体２０からソフトウェアＳｏｆｔＡに関する情報を獲得すると（ステップＳ３０１）、第１の復号部２３において、乱数Ｒによって、暗号化補助鍵Ｅ（Ｒ，ＲＡ）を復号し、補助鍵ＲＡを得る（ステップＳ３０２）。続いて、実行器２１は、第２の復号部２４において、この補助鍵ＲＡにより、暗号化ソフト鍵／実行回数Ｅ（ＲＡ，（ＫＡ，ｎＡ））を復号し、ソフト鍵ＫＡ及び実行回数ｎＡを得る（ステップＳ３０３）。さらに、実行器２１は、第３の復号部２５において、ソフト鍵ＫＡにより、暗号化ソフトＥ（ＫＡ，Ｓｏ

ｆｔＡ）を復号し、ソフトウェアＳｏｆｔＡを得る（ステップＳ３０４）。同時に、実行器２１は、実行回数検査部２６において、実行回数ｎＡが１以上であるか否かを検査し（ステップＳ３０５）、ｎＡが１以上であればソフト実行部２９に対して実行ＯＫを通知し、この通知を受けて、ソフト実行部２９はソフトウェアＳｏｆｔＡを実行する（ステップＳ３０６）。この後、実行回数更新部２７は、実行回数ｎＡを１減少してｎＡ’（＝ｎＡ－１）に更新する（ステップＳ３０７）。実行回数ｎＡ’は、第１の暗号部２８において、ソフト鍵ＫＡと共に補助鍵ＲＡで暗号化され（ステップＳ３０８）、この暗号化ソフト鍵／実行回数Ｅ（ＲＡ，（ＫＡ，ｎＡ’））が、記録媒体２０に再び格納される（ステップＳ３０９）。ソフトウェアＳｏｆｔＢについても、同様にして実行される。

【０００７】

このシステムは、ソフトウェアの実行後、所定のタイミングで乱数Ｒ、及び暗号化補助鍵Ｅ（Ｒ，ＲＡ）、Ｅ（Ｒ，ＲＢ）を更新する。図７は、この更新の際の、ソフトウェア実行システムの構成を示すブロック図である。図７において、記録媒体２０は、図５におけるものと同様の情報を格納している。実行器２１は、図５におけるものに加えて、第４の復号部３０と、乱数更新部３１と、第２の暗号部３２とを更に含むが、図には必要な部分だけが表示されている。

【０００８】

【発明が解決しようとする課題】

前述した従来例では、ソフト鍵、実行回数とも暗号化されているため、その編集ができず、ソフトウェアの不正使用、すなわちデジタルコンテンツの不正利用を防ぐことができた。しかしＥ（ＲＡ，（ＫＡ，ｎＡ））をバックアップし、何回かのソフトウェア実行後リストアするという攻撃が可能である。

【０００９】

この攻撃を繰り返すことにより、実行回数を暗号化して保持しておくことが無意味となり、永久に利用できてしまうという欠点を持つ。

【００１０】

本発明はこの問題を鑑み、たとえ何らかのデータ、例えば前述の従来例では暗号化ソフト鍵／実行回数や、一般的なデジタルコンテンツにおける利用条件など

をバックアップし、デジタルコンテンツの利用後リストアする攻撃に対しても、不正な利用ができないシステムを提供することを目的とする。

【００１１】

【課題を解決するための手段】

この課題を解決するために本発明は、デジタルコンテンツの利用に連携して、新たな補助鍵を生成する補助鍵生成手段と、新たに生成された補助鍵を用いて利用条件を暗号化する第１の暗号手段を備えたものである。

【００１２】

すなわち本発明は、予め定められた利用条件に従ってデジタルコンテンツの利用を制御し、かつ当該利用条件の不正な使用を防止するためのデジタルコンテンツ利用制御システムであって、複数の、デジタルコンテンツ、暗号化された利用条件及び暗号化された補助鍵を格納し、かつ情報の読み出し及び書き込みが可能な記録媒体が、デジタルコンテンツを実行する実行器に情報伝達可能に接続され、実行器は、乱数を格納し、かつ自己の外部からは情報の読み出し及び書き込みが困難な乱数格納手段と、記録媒体から暗号化された補助鍵を獲得して、乱数格納手段から取得した乱数で復号する第１の復号手段と、記録媒体から暗号化された利用条件を獲得して、第１の復号手段の復号によって得られた補助鍵で復号する第２の復号手段と、記録媒体から対応するデジタルコンテンツを獲得して、第２の復号手段の復号によって得られた利用条件に従って利用を実行するデジタルコンテンツ利用手段と、デジタルコンテンツの利用に連携して、新たな補助鍵を生成する補助鍵生成手段と、第２の復号手段の復号によって得られた利用条件を、デジタルコンテンツ利用に連携して、補助鍵生成手段によって得られた新たな補助鍵で暗号化して、記録媒体に格納する第１の暗号化手段と、デジタルコンテンツの利用に連携して、記録媒体から全ての暗号化された補助鍵を獲得して、乱数格納手段に格納された乱数で復号する第３の復号手段と、第３の復号手段の復号に連携して、乱数格納手段に格納された乱数を更新する乱数更新手段と、第３の復号手段の復号によって得られた補助鍵のから、第１の復号手段の復号によって得られた補助鍵を除き、補助鍵生成手段によって生成された補助鍵を加えたものを、乱数更新手段によって更新された乱数で暗号化して、記録媒体に格納する

第２の暗号化手段とを備えている。

【００１３】

上記のように、本発明は、デジタルコンテンツを利用する実行器と、複数の、デジタルコンテンツ、暗号化された利用条件及び暗号化された補助鍵が格納された記録媒体とで構成される。最初、実行器に備えられた第１の復号手段は、記録媒体から、利用すべきデジタルコンテンツに対応する暗号化された補助鍵を獲得し、乱数格納手段に格納された乱数で復号して補助鍵を求める。次に、第２の復号手段は、記録媒体から当該デジタルコンテンツに対応する暗号化された利用条件を獲得し、第１の復号手段の復号によって求められた補助鍵で復号して、利用条件を得る。デジタルコンテンツ利用手段は、得られた利用条件に従って、当該デジタルコンテンツの利用を実行する。続いて、補助鍵生成手段は、新たな補助鍵を生成し、第１の暗号化手段は、補助鍵生成手段によって生成された新たな補助鍵で、得られた利用条件を暗号化して記録媒体に格納する。また、第３の復号手段は、デジタルコンテンツの利用実行に関連して、記録媒体から、全ての暗号化された補助鍵を獲得し、乱数格納手段に格納された乱数で復号して補助鍵を求める。第３の復号手段の復号に連携して、乱数更新手段は乱数格納手段に格納された乱数を更新する。第２の暗号化手段は、第３の復号手段の復号によって求められた補助鍵から第１の復号手段の復号によって得られた補助鍵を除き、補助鍵生成手段によって生成された補助鍵を加えたものを、更新された乱数で暗号化して記録媒体に格納する。

【００１４】

このように、一つの実行器で複数のデジタルコンテンツを取り扱う場合には、デジタルコンテンツ毎の利用条件をそれぞれに専用の補助鍵で暗号化し、さらに、これらの補助鍵を乱数で暗号化する。そして、デジタルコンテンツの実行に関連して乱数を更新することにより、正規の実行器以外の実行器でデジタルコンテ不正に実行されるのを防止することができる。また、取り扱うデジタルコンテンツの数に関わらず、使用する乱数は一つだけでよいため、乱数を格納するための読み出し及び書き込みが困難な記憶領域は、一つの乱数を格納するだけの大きさを備えればよい。

【００１５】

また本発明の別の構成では、前述の発明において、デジタルコンテンツの利用実行にともなって、第２の復号手段の復号によって得られた利用条件を更新する利用条件更新手段をさらに備え、第１の暗号化手段は、利用条件更新手段によって更新された利用条件を、補助鍵生成手段によって得られた新たな補助鍵で暗号化して、記録媒体に格納することを特徴としている。

【００１６】

このように、上記の発明では、利用条件更新手段が、デジタルコンテンツの利用実行にともなって利用条件を更新し、第１の暗号化手段は、利用条件更新手段によって更新された利用条件を、補助鍵生成手段で生成した新たな補助鍵で暗号化する。これにより、コピーされた利用条件の不正な使用、更新された利用条件の記録媒体への書き込み妨害、デジタルコンテンツ利用以前にバックアップされた暗号化利用条件の、不正なリストアを防止することができる。

【００１７】

【発明の実施の形態】

以下、本発明の実施の形態について添付図面を用いて説明する。

【００１８】

図１は、本発明の実施形態に係るデジタルコンテンツ利用制御システムの構成を示すブロック図である。図１において、本システムは、デジタルコンテンツを格納する記録媒体１００と、デジタルコンテンツの利用を実行する実行器２００とを備えている。実行器２００は、乱数格納部２０１と、第１の復号部２０２と、第２の復号部２０３と、第３の復号部２０４と、利用条件確認部２０５と、利用条件更新部２０６と、補助鍵生成部２０７と、第１の暗号部２０８と、デジタルコンテンツ利用実行部２０９と、実行器固有鍵格納部２１０を含む。

【００１９】

図２は、図１のデジタルコンテンツ利用制御システムの動作を示すフローチャートである。図２を用いて、図１に示すシステムの動作を説明する。記録媒体１００には、複数のデジタルコンテンツに関する情報が格納されている。ここでは二つの暗号化デジタルコンテンツＥ（ＳＫ，ＭｕｓｉｃＡ）、Ｅ（ＳＫ，Ｍｕｓ

ｉｃＢ）と、それぞれに関する情報として、暗号化利用条件Ｅ（ＫＡ，ＩｎｆｏＡ）、Ｅ（ＫＢ，ＩｎｆｏＢ）、暗号化補助鍵Ｅ（Ｒ，ＫＡ）、Ｅ（Ｒ，ＫＢ）とが、格納されている。ここでＳＫは実行器固有鍵、ＫＡ及びＫＢは、それぞれデジタルコンテンツＭｕｓｉｃＡ、ＭｕｓｉｃＢ固有の補助鍵、Ｒは乱数である。またＥ（Ｋ，Ａ）はＡをＫで暗号化したものを示している。

【００２０】

乱数格納部２０１は、外部から読み出し及び書き込みの困難な領域であり、乱数Ｒを格納している。また実行器固有鍵格納部２１０も外部から読みだし及び書き込み困難な領域であり、実行器固有鍵ＳＫを格納している。実行器２００は、記録媒体１００からデジタルコンテンツＭｕｓｉｃＡに関する情報を獲得すると（ステップＳ１０１）、第１の復号部２０２において、乱数Ｒによって、暗号化補助鍵Ｅ（Ｒ，ＫＡ）を復号し、補助鍵ＫＡを得る（ステップＳ１０２）。続いて、実行器２００は、第２の復号部２０３において、この補助鍵ＫＡにより、暗号化利用条件Ｅ（ＫＡ，ＩｎｆｏＡ）を復号し、利用条件ＩｎｆｏＡを得る（ステップＳ１０３）。さらに、実行器２００は、利用条件確認部２０５において、デジタルコンテンツＭｕｓｉｃＡの利用が可能か否かを利用条件ＩｎｆｏＡで確認する（ステップＳ１０４）。ここでデジタルコンテンツの利用が可能であれば第３の復号部２０４において、実行器固有鍵ＳＫにより、暗号化デジタルコンテンツＥ（ＳＫ，ＭｕｓｉｃＡ）を復号し、デジタルコンテンツＭｕｓｉｃＡを得て、同時にデジタルコンテンツ利用実行部２０９でデジタルコンテンツＭｕｓｉｃＡを利用する（ステップＳ１０５）。さらにこのデジタルコンテンツの利用実行と同時に、利用条件更新部２０６で利用条件ＩｎｆｏＡをＩｎｆｏＡ’に更新する（ステップＳ１０６）。また補助鍵生成部２０７でＫＡと異なる補助鍵ＫＡ’を生成する（ステップＳ１０７）。最後に更新された利用条件ＩｎｆｏＡ’が第１の暗号部２０８で補助鍵ＫＡ’を使って暗号かされ、この暗号化利用条件Ｅ（ＫＡ’，ＩｎｆｏＡ’）が、記録媒体１００に再び格納される（ステップＳ１０８）。デジタルコンテンツＭｕｓｉｃＢについても、同様に利用実行される。

【００２１】

図３は、本実施形態において、図１、図２に示したデジタルコンテンツＭｕｓ

ｉｃＡの利用後、乱数Ｒを更新する際の、デジタルコンテンツ利用制御システムの構成を示すブロック図である。図３において、記録媒体１００は、図１におけるものと同様の情報を格納している。実行器２００は、図１におけるものに加えて、第４の復号部２１１と、乱数更新部２１２と、第２の暗号部２１３とを更に含むが、図３には乱数の更新に必要な部分だけが表示されている。

【００２２】

図４は、図３に示すシステムの、デジタルコンテンツＭｕｓｉｃＡの利用後、乱数Ｒを更新する際の動作を示すフローチャートである。図４を用いて、図３に示すシステムの動作を説明する。実行器２００は、記録媒体１００から暗号化補助鍵Ｅ（Ｒ，ＫＡ）及びＥ（Ｒ，ＫＢ）を獲得する（ステップＳ２０１）。そして第４の復号部２１１において乱数Ｒで復号して、補助鍵ＫＡ及びＫＢを得る（ステップＳ２０２）。この際、実行器２００は、乱数更新部２１２において、乱数格納部２０１に格納された乱数ＲをＲ’に更新する（ステップＳ２０３）。また獲得した補助鍵からデジタルコンテンツＭｕｓｉｃＡの利用条件復号に使われた補助鍵ＫＡを除き、補助鍵生成部で生成された新たな補助鍵ＫＡ’を加える（ステップＳ２０４）。続いて、実行器２００は、第２の暗号部２１３において、乱数Ｒ’で補助鍵ＫＡ’及びＫＢをそれぞれ暗号化し（ステップＳ２０５）、これらの暗号化補助鍵Ｅ（Ｒ’，ＫＡ’）及びＥ（Ｒ’，ＫＢ）を記録媒体２０に再び格納する（ステップＳ２０６）。

【００２３】

このように、本実施形態では、利用条件を暗号化するための各デジタルコンテンツ毎の補助鍵と、それらの補助鍵を束ねてそれぞれ暗号化するための乱数Ｒとを用意して、乱数格納部には乱数Ｒだけを格納するようにしている。このため、読み出し及び書き込みのできない領域の大きさを最小にすることができて、実現コストも低く抑えることができる。

【００２４】

また利用条件の更新に伴って、その暗号化に使う補助鍵も更新しているため、暗号化利用条件のみ過去にバックアップしたものをリストアして不正利用するという攻撃を防いでいる。また利用条件と補助鍵のペアを、過去にバックアップし

たものをリストアして不正利用しようとしても、補助鍵を束ねて暗号化する乱数も更新していることにより防御している。

【００２５】

【発明の効果】

以上のように本発明によれば、利用条件を不正に複製すること、更新後の利用条件の書き込み妨害に加え、過去の利用条件のバックアップの不正なリストアも防止することができ、その効果は大きい。

【図面の簡単な説明】

【図１】

本発明の実施形態に係わるデジタルコンテンツ利用制御システムの、デジタルコンテンツを利用する際の構成を示すブロック図

【図２】

図１のデジタルコンテンツ利用制御システムの動作を示すフローチャート

【図３】

本発明の実施形態に係わるデジタルコンテンツ利用制御システムの、乱数を更新する際の構成を示すブロック図

【図４】

図３のデジタルコンテンツ利用制御システムの動作を示すフローチャート

【図５】

特開平９－１８５５０１号公報に示されたソフトウェア実行制御システムの、ソフトウェアを実行する際の構成を示すブロック図

【図６】

図５のソフトウェア実行制御システムの動作を示すフローチャート

【図７】

特開平９－１８５５０１号公報に示されたソフトウェア実行制御システムの、乱数を更新する際の構成を示すブロック図

【符号の説明】

１００，２０　記録媒体

２００，２１　実行器

２０１　乱数格納部

２０２　第１の復号部

２０３　復号部

２０４　第３の復号部

２０５　利用条件確認部

２０６　利用条件更新部

２０７　補助鍵生成部

２０８　第１の暗号部

２０９　利用実行部

２１０　実行器固有鍵格納部

２１１　第４の復号部

２１２　乱数更新部

２１３　第２の暗号部

２２　乱数格納部

２３　第１の復号部

２４　第２の復号部

２５　第３の復号部

２６　実行回数検査部

２７　実行回数更新部

２８　第１の暗号部

２９　ソフト実行部

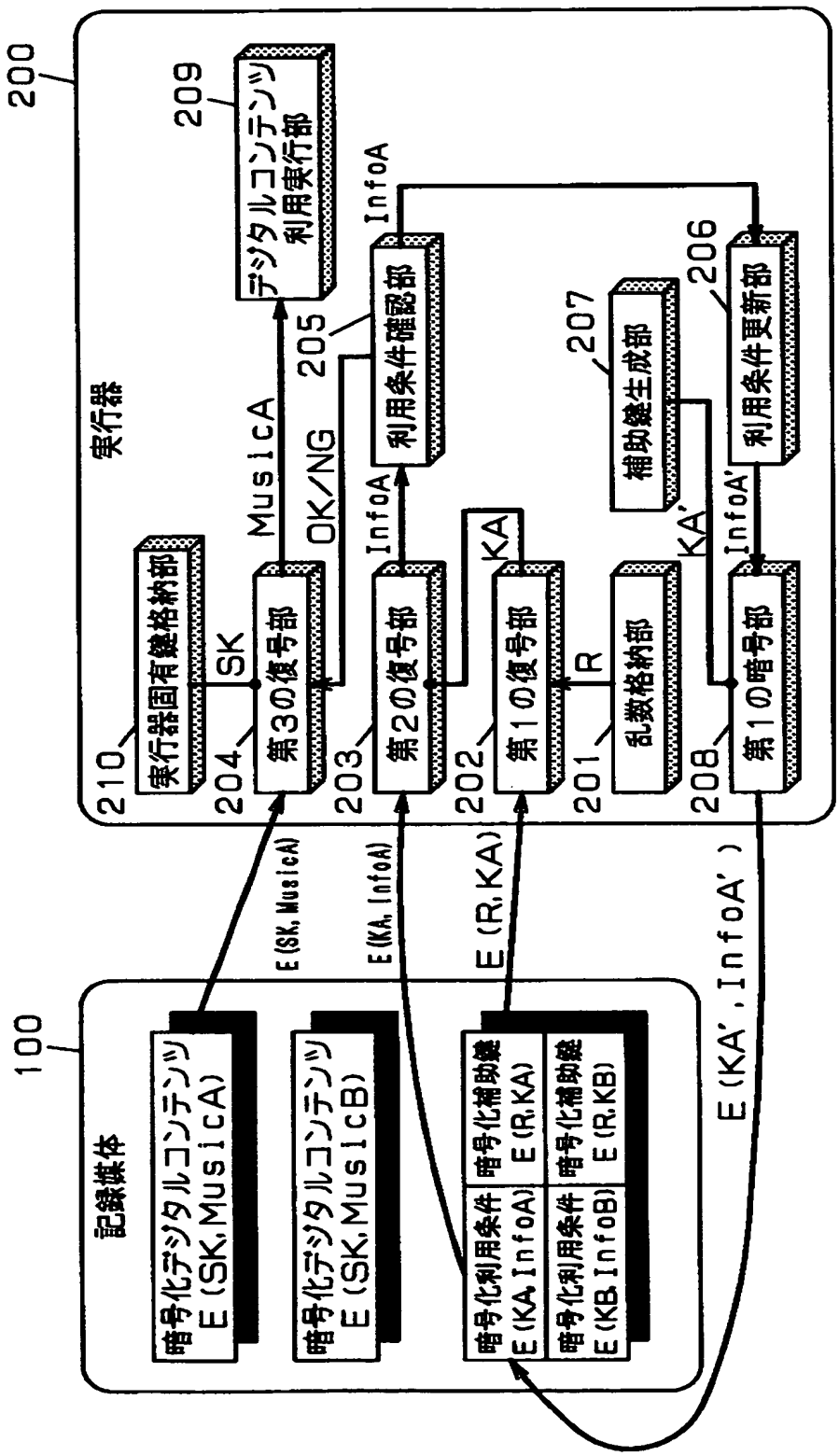
３０　第４の復号部

３１　乱数更新部

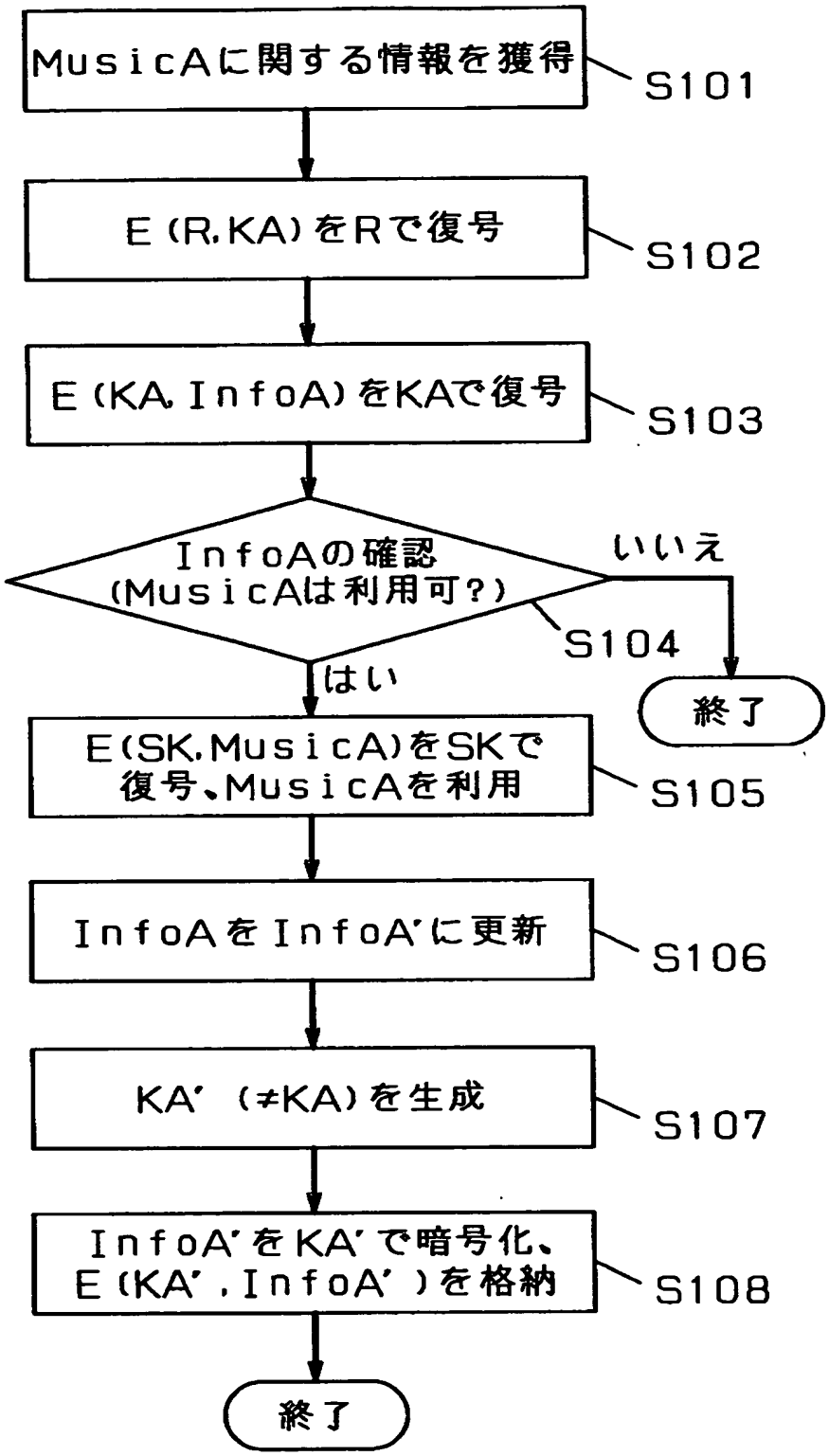
３２　第２の暗号部

【書類名】　　図面

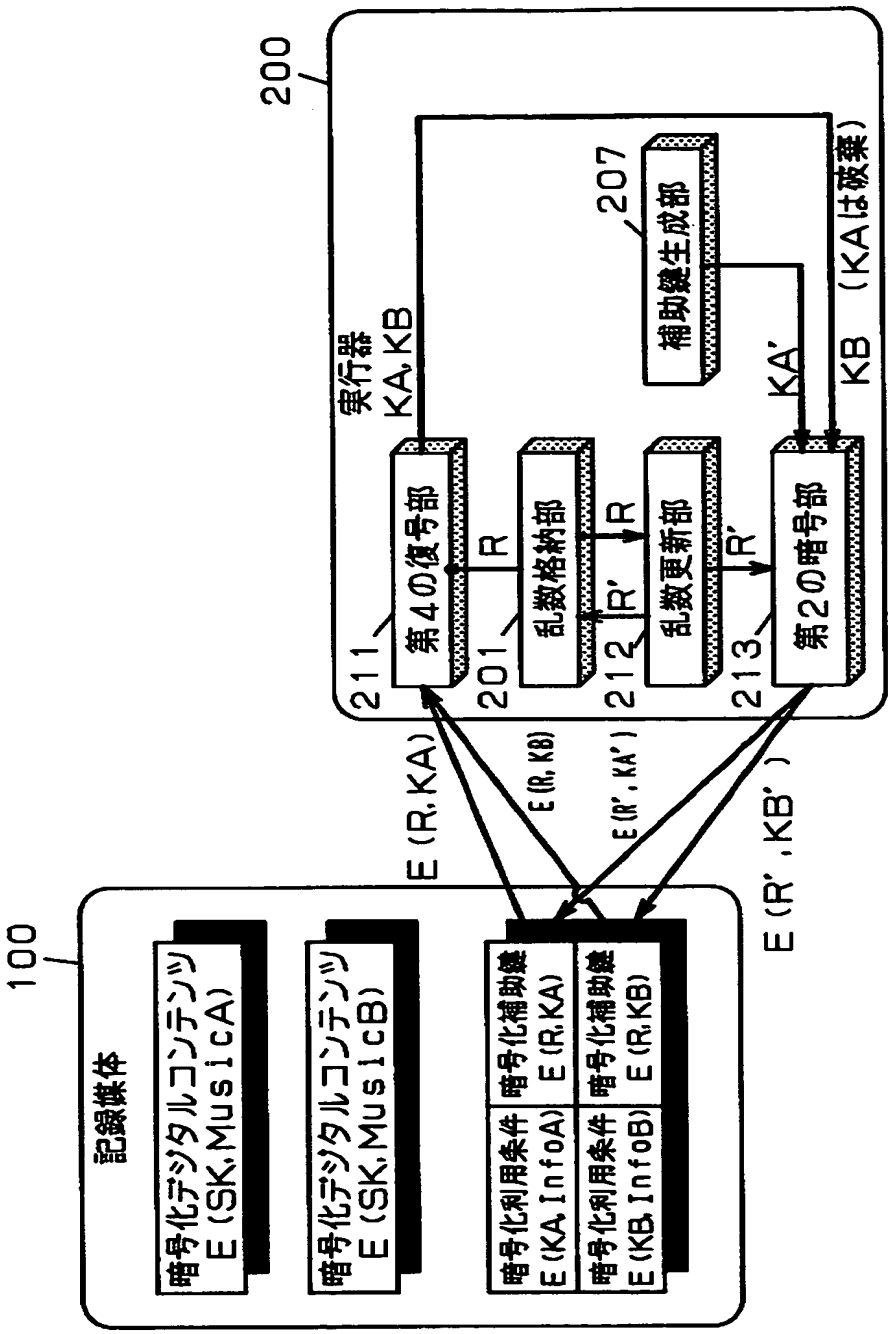
【図１】


200
実行器
209
デジタルコンテンツ利用実行部
InfoA
205
利用条件確認部
206
利用条件更新部
207
補助鍵生成部
MusicA
OK/NG
InfoA
KA
KA'
InfoA'
SK
R
210
実行器固有鍵格納部
204
第3の復号部
203
第2の復号部
202
第1の復号部
201
乱数格納部
208
第1の暗号部
E(SK, MusicA)
E(KA, InfoA)
E(R, KA)
E(KA', InfoA')
100
記録媒体
暗号化デジタルコンテンツ E(SK, MusicA)
暗号化デジタルコンテンツ E(SK, MusicB)
暗号化利用条件 E(KA, InfoA)
暗号化補助鍵 E(R, KA)
暗号化利用条件 E(KB, InfoB)
暗号化補助鍵 E(R, KB)

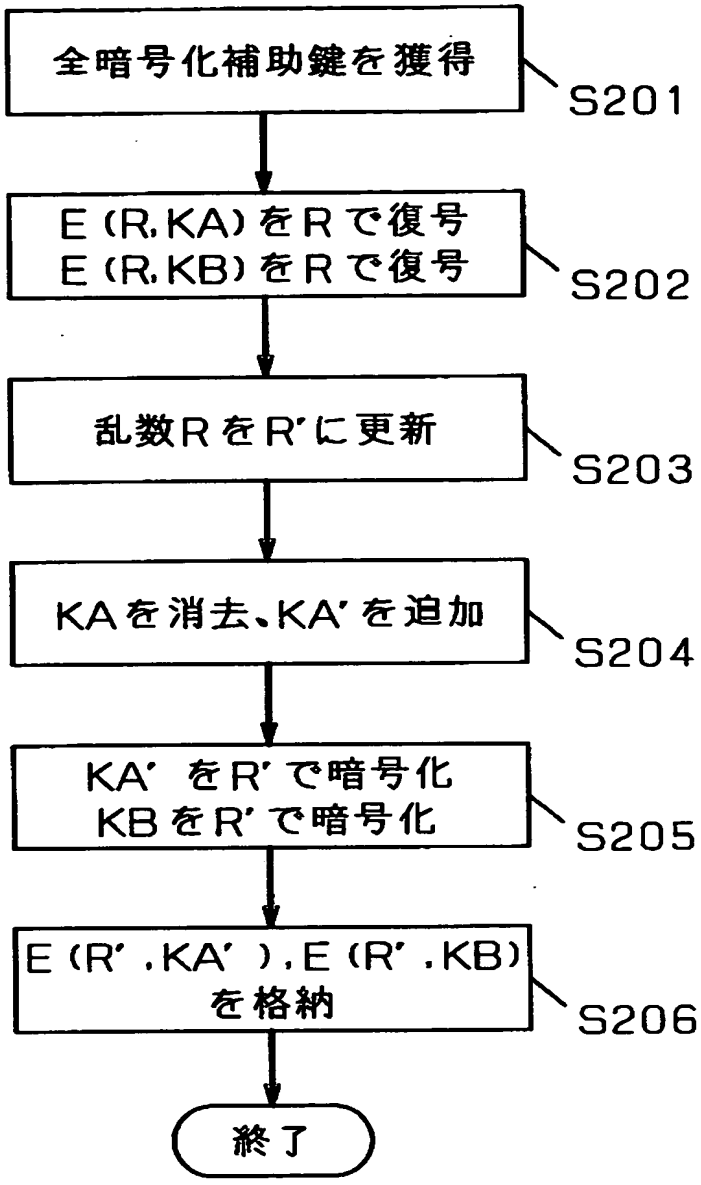
【図２】


MusicAに関する情報を獲得
S101
E(R,KA)をRで復号
S102
E(KA,InfoA)をKAで復号
S103
InfoAの確認
(MusicAは利用可?)
S104
いいえ
終了
はい
E(SK,MusicA)をSKで
復号、MusicAを利用
S105
InfoAをInfoA'に更新
S106
KA' (≠KA)を生成
S107
InfoA'をKA'で暗号化、
E(KA',InfoA')を格納
S108
終了

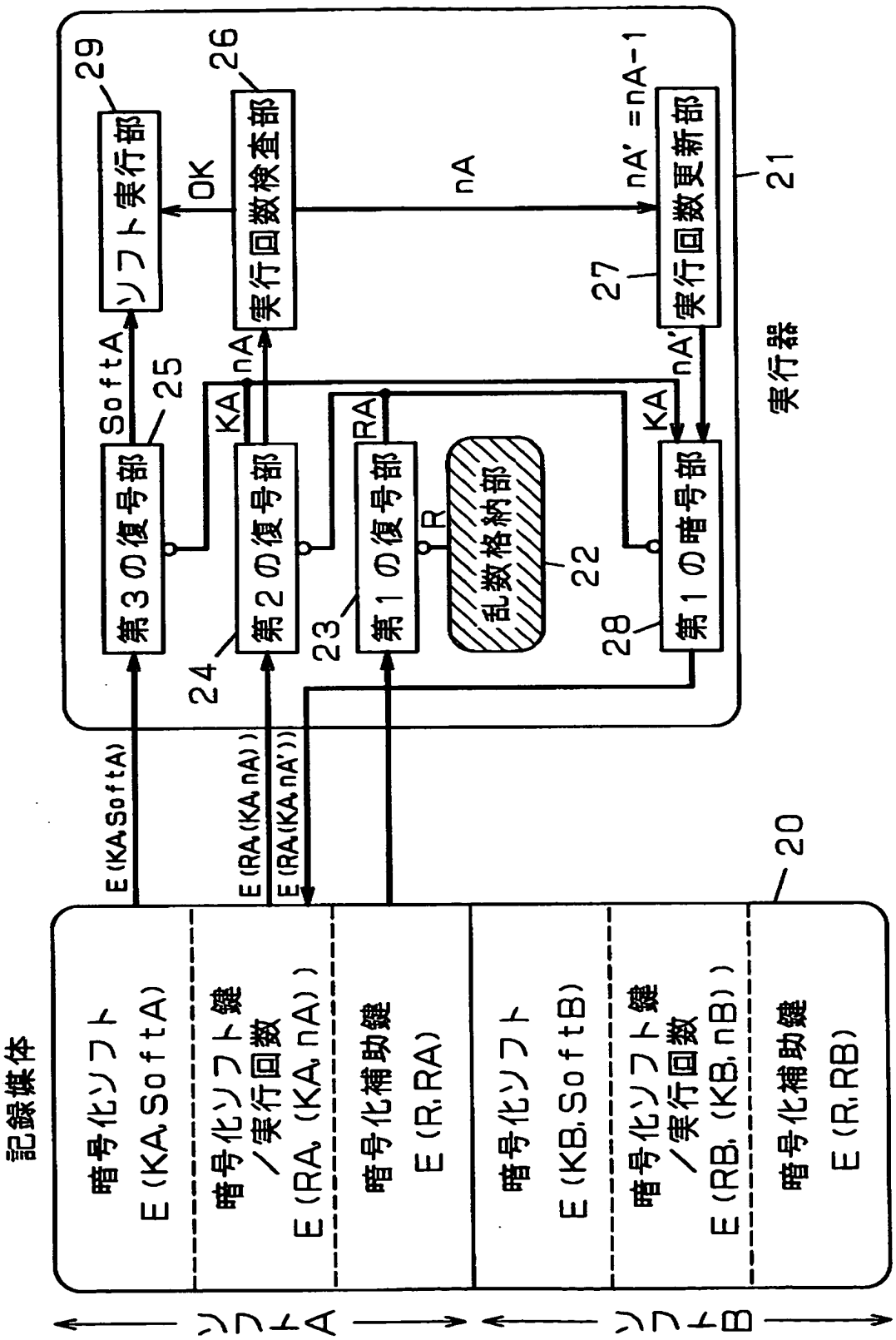
【図３】


100
記録媒体
暗号化デジタルコンテンツ E(SK,MusicA)
暗号化デジタルコンテンツ E(SK,MusicB)
暗号化利用条件 E(KA,InfoA)
暗号化補助鍵 E(R,KA)
暗号化利用条件 E(KB,InfoB)
暗号化補助鍵 E(R,KB)
200
実行器
KA,KB
211
第４の復号部
201
乱数格納部
212
乱数更新部
213
第２の暗号部
207
補助鍵生成部
KA'
KB (KAは破棄)
R
R'
R
R'
E(R,KA)
E(R,KB)
E(R',KA')
E(R',KB')

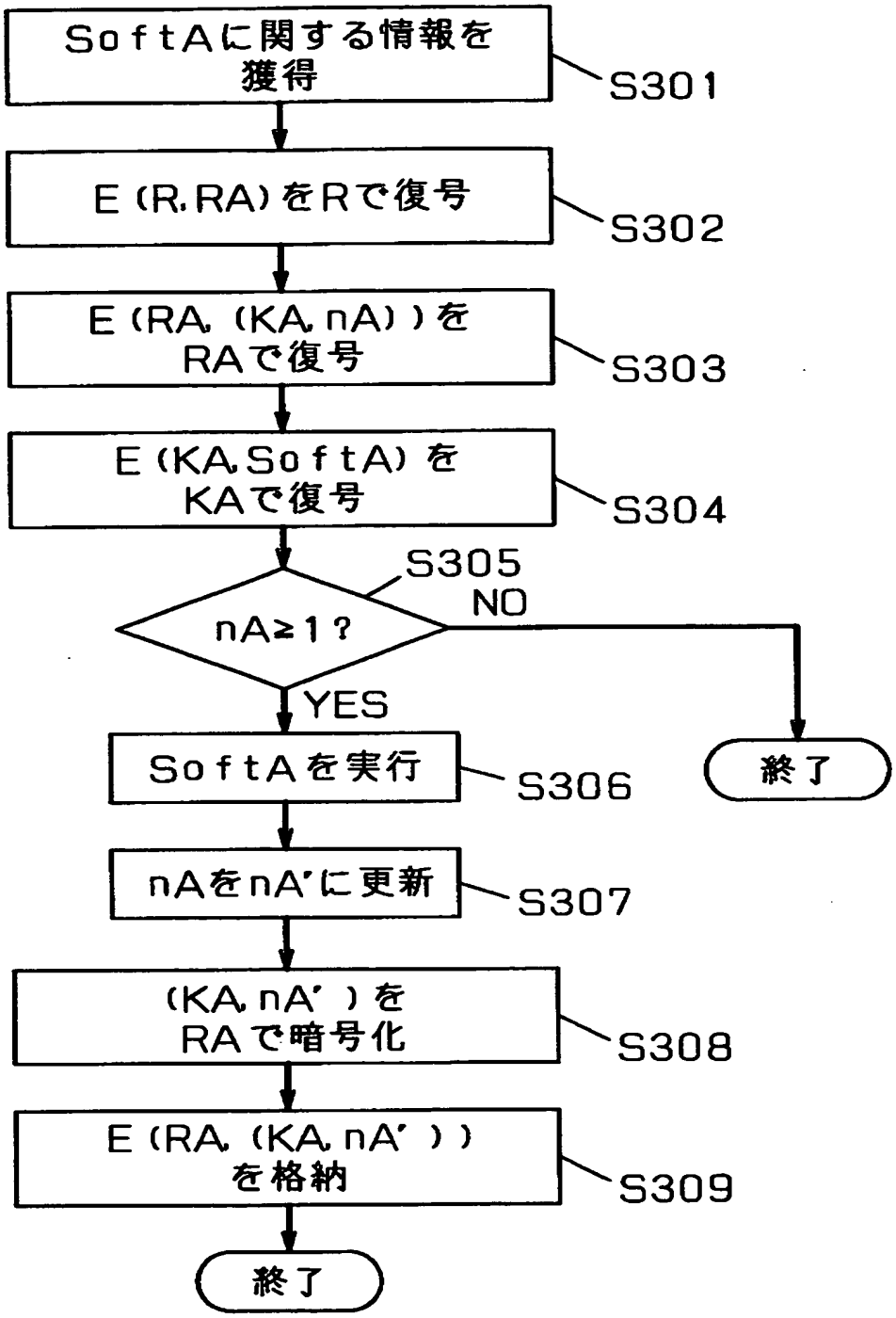
【図４】


全暗号化補助鍵を獲得
S201
E(R,KA)をRで復号
E(R,KB)をRで復号
S202
乱数RをR'に更新
S203
KAを消去、KA'を追加
S204
KA' をR'で暗号化
KBをR'で暗号化
S205
E(R',KA'),E(R',KB)
を格納
S206
終了

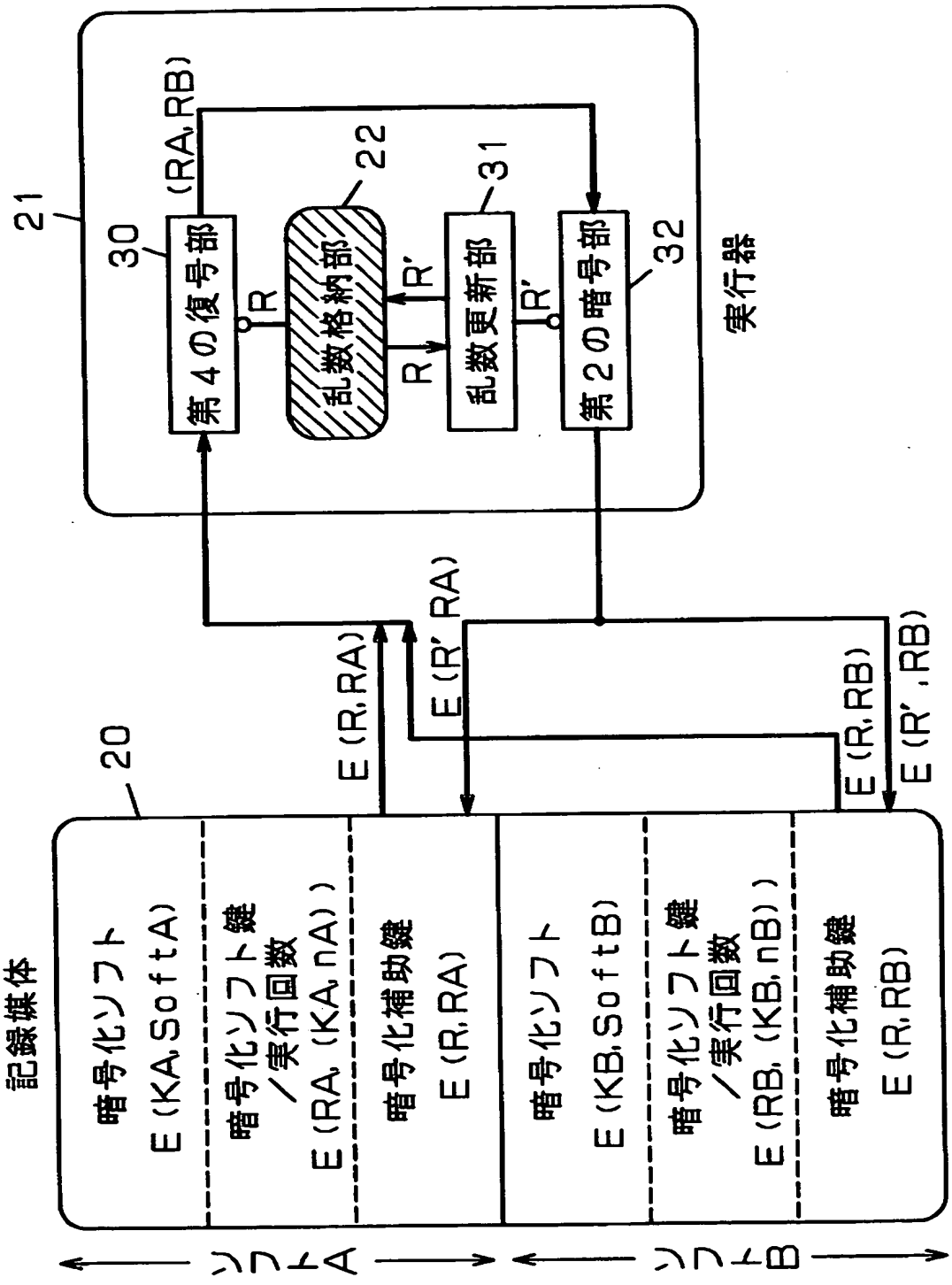
【図５】


記録媒体
暗号化ソフト
E(KA,SoftA)
暗号化ソフト鍵
／実行回数
E(RA,(KA,nA))
暗号化補助鍵
E(R,RA)
暗号化ソフト
E(KB,SoftB)
暗号化ソフト鍵
／実行回数
E(RB,(KB,nB))
暗号化補助鍵
E(R,RB)
ソフトA
ソフトB
20
E(KA,SoftA)
E(RA,(KA,nA))
E(RA,(KA,nA'))
実行器
21
第３の復号部
25
第２の復号部
24
第１の復号部
23
乱数格納部
22
第１の暗号部
28
ソフト実行部
29
実行回数検査部
26
実行回数更新部
27
SoftA
KA
nA
RA
R
OK
nA
nA'
nA'=nA-1

【図６】


SoftAに関する情報を獲得
S301
E(R,RA)をRで復号
S302
E(RA,(KA,nA))をRAで復号
S303
E(KA,SoftA)をKAで復号
S304
S305
nA≧1?
NO
YES
終了
SoftAを実行
S306
nAをnA'に更新
S307
(KA,nA')をRAで暗号化
S308
E(RA,(KA,nA'))を格納
S309
終了

【図７】


21
30
第４の復号部
(RA,RB)
R
22
乱数格納部
R'
R
31
乱数更新部
R'
32
第２の暗号部
実行器
E(R,RA)
E(R'RA)
E(R,RB)
E(R',RB)
20
記録媒体
暗号化ソフト
E(KA,SoftA)
暗号化ソフト鍵
／実行回数
E(RA,(KA,nA))
暗号化補助鍵
E(R,RA)
暗号化ソフト
E(KB,SoftB)
暗号化ソフト鍵
／実行回数
E(RB,(KB,nB))
暗号化補助鍵
E(R,RB)
ソフトA
ソフトB

【書類名】　要約書

【要約】

【課題】　利用条件によりデジタルコンテンツの利用制御を行なうデジタルコンテンツ利用制御システムにおいて、利用条件をバックアップし、デジタルコンテンツの利用後リストアすることによる不正利用を防ぐことを目的とする。

【解決手段】　補助鍵更新手段を設け、利用条件の更新に連携し、利用条件を暗号化する際に用いる補助鍵も更新する。さらに補助鍵は外部から読み書き不能な乱数によって暗号化する。

【選択図】　図１

出　願　人　履　歴　情　報

識別番号　　〔０００００５８２１〕

１．変更年月日　　１９９０年　８月２８日
［変更理由］　新規登録
住　所　大阪府門真市大字門真１００６番地
氏　名　松下電器産業株式会社